UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

MOOG INC.,

Plaintiff,

v.

Case No.: No. 22-cv-00187

SKYRYSE, INC., ROBERT ALIN PILKINGTON, MISOOK KIM, and DOES NOS. 1-50,

Defendants.

DECLARATION OF BRUCE W. PIXLEY

BRUCE W. PIXLEY, under penalty of perjury and pursuant to 28 U.S.C. § 1746, declares the following to be true and correct:

IV. Background

1. My name is Bruce W. Pixley. I provide this declaration in support of Moog Inc.'s ("Moog") Motion to Compel Discovery Necessary for Further Trade Secret Identification. I am over the age of 18 years. I have personal knowledge of the matters set forth herein and if called as a witness, I could and would competently testify as to all facts set forth herein.

2. I am the Managing Member of Pixley Forensics Group LLC. My responsibilities include assisting corporate clients and law firms in investigations and disputes involving forensic accounting issues, electronic discovery, theft of intellectual property, and computer forensic investigations. In this capacity, I manage teams of forensic examiners and use a variety of technologies to perform data acquisition and analysis of this information.

3. Since 2001, I have served as a lead instructor of computer forensics, Internet investigations, and network intrusion courses for the California Department of Justice's Advanced Training Center. Additionally, I have been employed as a Master Instructor at Guidance Software, which developed the EnCase computer forensic software. As an instructor, I have taught for over 2,000 hours on the subjects of computer forensics and high-tech investigations. I have developed course training materials and wrote manuals for computer forensic courses such as Advanced Internet Examinations and Network Intrusion Investigations.

4. I possess three professional certifications for my fields of work. I possess the Certified Information Systems Security Professional (CISSP) certification and the GIAC Certified Forensic Analyst (GCFA) certification, which are both ANSI ISO accredited credentials, and the EnCase Certified Examiner certification.

5. Since 2003, I have been retained as a computer forensic examiner and subject matter expert in both criminal and civil matters. I have been qualified as an expert witness in both state and federal courts and testified about the foundation of computer forensics, Windows and Mac operating systems, chat software, Internet and network operations, e-mail, peer-to-peer file sharing, digital photography, recovery of deleted data, and Trojan viruses.

6. I have been retained by Sheppard, Mullin, Richter & Hampton LLP, counsel for Moog Inc. (“Moog” or “Company”) to conduct a forensic analysis of: 1) certain company-issued laptop computers and external storage drives for any evidence of the exfiltration of Company data; and 2) electronic devices and data produced by the Defendants in this case which are in the possession of a third party forensics vendor, iDiscovery Solutions (“iDS”).

V. iDS Devices That Have Not Been Made Available for Review/Inspection

7. Pursuant to the procedures set forth in the Protective Order entered in this case (ECF 89) and the Inspection Protocol (ECF 96-02), I have been granted access to certain electronic devices turned over to iDS through inspection laptops and iDS' remote virtual machine software.

8. iDS has created an inventory of forensic images of electronic devices turned over by the Parties in this case. To date, I have not been granted any access to forensic images identified as Device Nos. E0005, 10, 18, 19, 23, and 25.

9. Based on the inventory and list of electronic devices provided by iDS, I understand that the Serial Number for Device E0018 is AFDD0200107304 and the Serial Number for Device E0019 is S5SCNS0R700159M.

10. As part of my initial investigation and analysis of digital evidence in this matter, I received and analyzed a forensic image of the Dell Precision laptop assigned to defendant Alin Pilkington ("Pilkington") while he worked at Moog. I found that Pilkington had used two USB storage devices prior to his departure from Moog. One device was a Samsung USB device (the "Samsung Device") and the other was a Buffalo USB device (the "Buffalo Device"). Both of these devices contained Moog data and are the same devices identified in paragraph 9 above.

a. On September 10, 2021, at 1:31 pm, Pilkington plugged in the Samsung Device for the first time and copied Moog data to this device. This device was used with his Moog laptop until his departure on November 12, 2021. This same Samsung Device had been used in defendant Misook Kim's Moog-issued laptop from September 2021 through the end of November 2021.

b. On October 27, 2021, at 9:40 a.m., Pilkington plugged in the Buffalo Device for the first time and copied over 1 million files and folders to this device, which was effectively a complete backup of his Moog laptop. On November 12, 2021, he created an updated copy of data from his Moog laptop to a folder called "11-12-2021." This device was used with his Moog laptop until his departure on November 12, 2021.

11. E0005 is defendant Kim's personal Windows computer that she turned over to iDS. In my declaration dated March 7, 2022 (ECF 4-28), I described the events surrounding Kim's action of taking Moog data using a Samsung USB storage device, which was formatted for use on a Windows-based computer. The Samsung storage device was returned to Moog, which I found had been wiped and formatted. As stated in my declaration: "Since the Samsung USB Storage 1 device was formatted and wiped, I am unable to determine: a) What computers the device may have been connected to after December 17, 2021; and b) When or how anyone may have accessed, copied, transferred, modified, or otherwise exported the data on the drive after it was removed from Moog on December 17, 2021." (ECF 4-28, ¶ 30). Device E0005 is a personal Windows computer belonging to Kim which could provide insight into answering these two critical questions regarding Moog's data.

12. E0023 is another one of Pilkington's USB drives that he turned over to iDS for inspection. E0010 is another one of Kim's USB devices that she turned over to iDS for inspection. During my analysis, I found that both Pilkington and Kim actively used USB storage devices to copy Moog's data prior to their departure from Moog. E0023 is the same make and model (Buffalo, SSD-PG1) as the drive he used to copy his entire Moog laptop on October 27, 2021 (identified in Paragraph 10 above). In my experience it is common for people to use external USB storage drives to backup data. Based on my experience and analysis of the actions of Pilkington and Kim, and the devices they used, there is a reasonable likelihood that Devices E0023 and/or E0010 contain evidence of storage and/or use of Moog data.

VI. Issues Related to SanDisk Cruzer Devices

13. I have reviewed Skyryse's May 4, 2022 letter (ECF 169-01) (the "May 4 Letter"). Therein Skyryse acknowledges that "it appears that Moog information may have been accessed

on Skyryse-issued laptops via personal USB devices held by Alin Pilkington or Misook Kim." (p. 6). Skyryse then provided a table on page 7 that apparently "reflects connection to SanDisk Cruzer devices that, based on the index prepared by iDS and shared with the parties, may have been delivered to iDS by individual defendants Misook Kim and Alin Pilkington."

14. In the table on page 7 of the May 4 Letter, there are three external drive devices for which Skyryse provided VSN (Volume Serial Numbers): 55D28D65, 80FC319F, and EC979D10. Skyryse did not provide any VSN for device connections involving computer Host Serial FM1W5J3. According to Skyryse May 4 Letter, this computer belongs to Skyryse employee and custodian Sathya Achar.

15. Based on my review of the electronic devices made available by iDS, as well as the inventory of devices prepared by iDS, there were only two SanDisk devices that were turned over by Kim (iDS Devices Nos. E0013 and E0024). Only one of the two SanDisk devices (E0013) matches one of the VSNs (80FC319F) in Skyryse's chart on page 7 of the May 4 Letter.

16. Kim wiped device E0013 on May 10, 2022, so there is no recoverable data on that drive. During my analysis of the forensic image associated with this device, I found that the device had been formatted with the NTFS file system. This file system maintains hidden files and the creation dates of these files are when the device was formatted (March 10, 2022). This action is similar to the wiped Samsung drive that Kim returned to Moog. As I described in my March 7, 2022 declaration: "This process was intentional, destructive, and obscured my ability to recover any data on the drive. When a hard drive is formatted, it needs to be connected to a computer to start and complete the process. At the start of the formatting process, a user has choices to set options on how the drive will be formatted. In this case, the user selected the option to force the formatting process to overwrite and wipe all sectors on the drive with zeroes.

Not only is formatting a drive an intentional act, but this specific formatting process effectively wiped all previous data on the drive so all previous data would be unrecoverable." (ECF 4-28, ¶ 29). That same drive (E0013) was plugged into Skyryse employee Mario Brenes' computer (Host Serial: J54MD5K) on February 18, 2022.

17. The following computers listed on page 7 of the May 4 Letter as having been connected to the SanDisk Cruzer devices at issue have not been turned over to iDS and have not been made available for inspection/review:

- Dell Latitude 9520 belonging to Sathya Achar (Host Serial FM1W5J3);
- Dell Latitude 9520 belonging to Mario Brenes (Host Serial J54MDK);
- Dell Latitude 9520 belonging to Lawrence Chow (Host Serial HSYLDK3);
- Dell Latitude 9520 belonging to Eric Chung (Host Serial C1DD6J3);
- Dell Latitude 9520 belonging to Santiago Correa-Mejia (Host Serial 174LDK3);
- Dell Latitude 9520 belonging to Tri Dao (Host Serial JGNV5J3);
- Dell Latitude 9520 belonging to Cynthia Le (Host Serial 4S8LDK3);
- Dell Latitude 9520 belonging to John Stafford (Host Serial CRGD6J3); and
- Dell Latitude 9520 belonging to Alex Wang (Host Serial 80RMDK).

18. The May 4 Letter from Skyryse limited its information to three SanDisk USB storage devices and failed to list any other USB storage devices connected to Skyryse employee computers. In this matter, USB storage devices have been the primary method to copy and take Moog data. Thus, inspection of these 9 computers is important to determining whether Moog data was transferred to them from the various USB storage devices used by Kim and Pilkington, as well as understanding the connection history with such devices.

VII. Additional Issues Preventing Full Access to iDS Devices

19. To date, iDS has not included or made available "Volume Shadow Copies" for certain of the electronic devices. "Volume Shadow Copies" are periodic backups that are generated and stored by Windows laptops. These backups essentially contain copies of files stored on the hard drive at a specific time that have been subsequently modified or deleted.

20. During my analysis of Kim's Skyryse-issued laptop (Device E0001), I found that Kim deleted what appears to be approximately 780 Moog files from her Skyryse-issued Windows laptop. During my analysis I found deleted file records that provided the file name, file size, and date/time stamps, such as those pertaining to when files are created and modified. However, the contents of these files have been deleted. The only available method to review the contents of these deleted files (and to confirm that they are in fact Moog files) is by seeing if they can be recovered from the periodic backup "Volume Shadow Copies."

21. To my knowledge to date, this absence of "Volume Shadow Copies" impacts at least iDS Devices Nos. E0001 and E0027, but may include additional devices because I have not been granted access to all iDS devices yet.

22. Separately, certain of Defendants' devices have a virtual machine application called Parallels. Parallels is a commercially-available program that is specifically designed to run on an Apple computer. Parallels allows an Apple user to run a Windows-based operating system on their Apple computer. Each Parallels virtual machine stored on the Apple computer has a proprietary virtual hard drive, which is a large container-type file that mimics a hard drive. In addition to the virtual hard drives stored on the Defendants' devices, there are backup copies of the virtual hard drives stored on the Defendants' external hard drive. These proprietary virtual hard drives cannot be viewed or accessed through the iDS virtual machines because they are

Windows machines. This impacts at least Devices Nos. E0014, 0016, 0017, and 0028. These proprietary virtual hard drives need to be analyzed just like an ordinary forensic image of a computer. However, in order to view the proprietary virtual hard drives, the file must be converted to what Parallels refers to as a "plain" image format. This conversion process can only be accomplished using Parallels on an Apple computer. Once the proprietary virtual hard drive has been converted to "plain" image format, the image will be accessible just like the industry-standard forensic image provided by iDS. This conversion task must be handled by iDS. Once the proprietary virtual hard drives have been converted, Defendants will be able to conduct a privilege review just like the other images hosted by iDS.

VIII. Communications between Pilkington and Lori Bird

23. [redacted]

///

///

///

///

I declare that the foregoing is true and correct under penalty of perjury under the laws of the United States of America.

Dated: August 3, 2022

Bruce W. Pixley